

صنعت کارت و پرداخت

مفاهیم، روش ها و امنیت

آجای کومار

ثنا جهاندار



 IDPay

انتشارات راه پرداخت



انتشارات راه پرداخت

برای دانلود نسخه کامل به وبسایت
فروشگاه انتشارات راه پرداخت مراجعه کنید
way2pay.shop

نسخه نمونه

بسم الله
الرفيع
الرفيع

۱

۳

۹

۹

صنعت کارت و پرداخت

مفاهیم، روش ها و امنیت

 IDPay

انتشارات **راه پرداخت**

سرشناسه: کومار، آجای، ۱۹۶۲-م. / Kumar, Ajay, 1962- / عنوان و نام پدیدآور: صنعت کارت و پرداخت / نویسنده: آجای کومار؛ مترجم ثنا جهاندار؛ / مشخصات نشر: تهران: راه پرداخت، ۱۳۹۹. / مشخصات ظاهری: ۱۰۴ ص.؛ ۲۱/۵×۱۴/۵ س.م. / شابک: ۹۷۸-۶۲۲-۹۷۸۲۹-۴-۱ / وضعیت فهرست نویسی: فیپا / یادداشت: عنوان اصلی: Payment Card Domain Knowledge: Card terminology, processing & security / Bank credit cards / in PCI (Payment Card Industry) / موضوع: کارت‌های اعتباری بانکی / موضوع: Bank credit cards / موضوع: کارت‌های اعتباری بانکی - تدابیر ایمنی / موضوع: Bank credit cards - Security measures / موضوع: رمز ارز / موضوع: Cryptocurrencies / موضوع: بانکداری اینترنتی / موضوع: Internet banking / شناسه افزوده: جهاندار، ثنا، ۱۳۷۱-، مترجم / رده بندی کنگره: HG۳۷۵۵/۷ / رده بندی دیویی: ۳۳۲/۷۶۵ / شماره کتابشناسی ملی: ۷۵۳۸۷۷۹ / وضعیت رکورد: فیپا

چرا از کاغذ بالکی استفاده می‌کنیم؟

۱. کاغذ بالکی از کاغذهای تحریر سفید، سبک‌تر است
 ۲. در تهیه آن از مواد شیمیایی استفاده نشده و شیوه تولید آن مکانیکال است
 ۳. نور را منعکس نمی‌کند و مانع از خستگی چشم هنگام مطالعه می‌شود
- * کاغذ بالکی به دلیل موارد بالا از کاغذ تحریر سفید گران‌تر است



The mark of
responsible forestry
FSC® C009732

این کتاب با کاغذ بالکی دوستدار محیط زیست تولید شده است.

صنعت کارت و پرداخت

مفاهیم، روش ها و امنیت

نویسنده:

آجای کومار

مترجم:

ثنا جهاندار

 IDPay

انتشارات **راه پرداخت**

صنعت کارت و پرداخت، مفاهیم، روش ها و امنیت / ناشر: راه پرداخت / نویسنده: آجای کومار / مترجم: ثنا جهاندار / ناظر
ارشد: مینا والی / ویراستار فنی: یلدا شایسته‌فر / صفحه‌آرا: علیرضا کیوان / نوبت چاپ: اول ۱۳۹۹ / شمارگان: ۱۰۰۰ نسخه
/ شابک: ۹۷۸-۶۲۲-۹۷۸۲۹-۴-۱ / تمام حقوق این اثر محفوظ و متعلق به موسسه انتشارات راه پرداخت است / تلفن:
۰۲۱-۴۴۴۴۳۹۶۶ / دورنگار: ۸۹۷۸۴۹۰۲ / ایمیل: press@way2pay.ir / وبسایت: Shop.Way2Pay.ir

فهرست

۱۵	بخش اول: درک اینکه کارت و پرداخت چگونه کار می کند
۱۶	۱. چگونه عملکرد تراکنش های پرداخت
۲۱	۲. داده ذخیره شده در یک کارت پرداختی
۲۷	۳. نهادهای دست اندرکار در اعطای اجازه قانونی به یک تراکنش پرداخت با کارت
۳۳	۴. دریافت پول؛ تصفیه و تسویه
۳۷	۵. تراکنش های تجارت الکترونیکی و ارائه دهندگان خدمات پرداخت
۴۲	۶. بازگردانی یک تراکنش؛ بازپرداخت و استرداد وجه
۴۶	۷. دریافت پول نقد از دستگاه خودپرداز
۵۱	بخش دوم: کدام استانداردهای صنعت کارت و پرداخت را به کار بگیریم؟
۵۲	۸. مجرمان چگونه از داده های کارت و پرداخت نفع می برند؟
۵۷	۹. از کجا داده ای پیدا کنیم که ارزش به سرقت بردن داشته باشد؟
۶۵	۱۰. تفاوت بین کارت های تراشه دار
۷۱	۱۱. استانداردهای صنعت پرداخت از کجا آمده اند؟
۷۶	۱۲. استاندارد امنیت داده و استاندارد امنیت داده برنامه های کاربردی پرداخت
۸۲	۱۳. استانداردهای امنیت تراکنش پین
۸۷	۱۴. استانداردهای PCIP2PE و تولید کارت
۹۱	۱۵. استانداردهای صنعت کارت و پرداخت را از کجا پیدا کنیم؟

[یادداشت حامی]

از زمان راه اندازی آیدی پی به همراه شرکای خودم مهم ترین دغدغه ام ایجاد تجربه های لذت بخش خدمات پرداخت بر بستر اینترنت در ایران بود؛ تجربه ای که بتواند در عین حال آسان تر، امن تر و سریع تر از روش های سنتی پرداخت باشد. مشکلات و موانعی را که همه کسب و کارها؛ اعم از آنلاین و غیر آنلاین در موضوعات مربوط به دریافت وجه از مشتری داشتند، از نزدیک مشاهده می کردم و این انگیزه ای جدی برای شکل گیری آیدی پی شد.

در روزهای اول آیدی پی که «درگاه پرداخت شخصی» مهمترین و اصلی ترین سرویس آیدی پی بود تا به امروز که با تمرکز بر توسعه سرویس های جدید در حوزه های گوناگون؛ کیف پول الکترونیکی، پرداخت از طریق QR Code و NFC و غیره مهم ترین سرویس های ما است، اصلی ترین دغدغه ما ارائه محصولی با کیفیت بوده که بتواند در کنار پشتیبانی ۲۴ ساعته، اطمینان خاطر را برای کاربرانمان ایجاد کند و آنها را راضی نگه دارد.

این سال ها هر اتفاق مثبتی را که در کسب و کارمان رخ داد، مدیون توجه دقیق به جزئیات، اشراف به مفاهیم فنی، رصد رقبای داخلی و خارجی، رصد ترندهای روز دنیا و تحقیق و توسعه مداوم در مورد صنعت پرداخت می دانیم که باعث خلق محصولات با کیفیت برای کاربرانمان شد.

کتاب پیش رو که توسط انتشارات راه پرداخت ترجمه و منتشر شده، کتابی بسیار

ارزشمند برای علاقه‌مندان و فعالان صنعت پرداخت است؛ چراکه فعالیت در هر حوزه‌ای بدون اطلاع از تاریخچه و جزئیات آن امکان‌پذیر نیست و چه بسا آگاهی از تاریخچه و جزئیات آن نیز ممکن است ما را با واقعیت‌های جدیدی آشنا کند و راهگشای ما در آینده باشد.

خواندن این کتاب به ما کمک می‌کند تا از جزئیات مهم و پشت پرده تراکنش‌های آنلاین یا فیزیکی آگاهی پیدا کنیم و با استانداردهای مختلف در این حوزه آشنا شویم. دانستن این جزئیات به فعالان این صنعت کمک می‌کند تا در فرایند توسعه محصولات خود چابکی بیشتری داشته باشند و تصمیمات دقیق‌تری در فرایند توسعه‌ای خود اتخاذ کنند.

به عنوان یک فعال صنعت فین‌تک در ایران، صمیمانه از مجموعه راه پرداخت بابت زحمات بسیار ارزشمندی که برای انتشار این اثر کشیده‌اند، قدردانی می‌کنم و امیدوارم این دست فعالیت‌ها ادامه‌دار باشد و با ترجمه آثار به روز دنیا بر کیفیت محصولات و خدمات این حوزه در داخل کشور بیفزاید.

قاسم رادمان
مدیرعامل آیدی پی

[یادداشت ناشر]

پرداخت با کارت‌های پلاستیکی از اواخر دهه ۸۰ به بخشی از زندگی ما تبدیل شد. تا پیش از آن، پول نقد به صورت سکه و اسکناس در کشورمان حرف اول را می‌زد؛ اما حالا در آستانه سال ۱۴۰۰ در کیف پول هر یک از ما چند کارت پلاستیکی وجود دارد و پرداخت با کارت به موضوعی کاملاً عادی و رایج تبدیل شده است؛ به طوری که در دورافتاده‌ترین روستاهای کشور نیز مردم برای پرداخت‌های خود از کارت استفاده می‌کنند.

با این حال مفاهیم فنی این حوزه چندان مورد توجه قرار نگرفته است. ما با کمبود شدید منابع آموزشی در زمینه کارت و پرداخت مواجه هستیم. مثلاً اینکه چه فرایندهایی در پس ماجرا رخ می‌دهد که ما بتوانیم با کشیدن یک کارت کالای مورد نظرمان را بخریم، همچنان برای خیلی‌ها ناشناخته و گنگ است. نه تنها برای مردمی که در صنعت کارت و پرداخت فعالیت نمی‌کنند؛ بلکه برای آنهایی هم که در این صنعت فعالیت می‌کنند، همه چیز روشن نیست. بارها پیش آمده که کسانی را دیده‌ایم که در نظرشان صنعت کارت و پرداخت را فعالیتی ساده و دم‌دستی می‌بینند. زیبایی صنعت پرداخت این است که بدون اینکه ذهن و فکر مردم را درگیر کند، پرداخت را به سادگی پردازش می‌کند. برای اینکه بدانید این صنعت چقدر در سال‌های گذشته پیشرفت کرده، کافی است یادمان بیاید که در سال‌های نه چندان دور چقدر مردم به این صنعت بی‌اعتماد بودند.

ناگفته نماند که در سایر نقاط دنیا نیز وضعیت، چندان بهتر از ایران ما نیست و اساساً

صنعت کارت و پرداخت حوزه‌ای است که کمتر به آن توجه شده است. کتابی که در دست دارید، از محدود کتاب‌هایی است که به‌طور خاص بر روشن کردن مفاهیم صنعت کارت و پرداخت متمرکز شده و تلاش کرده خلاء دانشی موجود در این حوزه را تا حدودی برطرف کند. این کتاب با استفاده از نمودارها و مثال‌های فراوان، توضیح می‌دهد که وقتی یک تراکنش به شکل آنلاین یا به‌صورت فیزیکی در یک فروشگاه انجام می‌شود، در پشت پرده چه اتفاقی می‌افتد و چه می‌شود که در نهایت، آن تراکنش، انجام می‌شود و پول از حساب ما کسر می‌شود. موضوع احراز هویت و همچنین استانداردهایی که در این صنعت وجود دارد، از جمله مباحث مهمی است که در این کتاب به آنها پرداخته شده است.

مطالعه این کتاب قطعاً می‌تواند به فعالان و علاقه‌مندان حوزه کارت و پرداخت کشور کمک کند تا بینش جامع‌تری نسبت به این حوزه پیدا کنند.

ما در مجموعه راه پرداخت انتشار کتاب‌های بیشتری در زمینه کارت و پرداخت را در برنامه داریم و امیدواریم بتوانیم قدمی هرچند کوچک در توسعه دانش فنی صنعت پرداخت کشور برداریم.

قاسم سرافرازی
انتشارات راه پرداخت

{

مقدمه

}

کتاب «همه چیز درباره کارت و پرداخت؛ مفاهیم، روش‌ها و امنیت در صنعت پرداخت» تمام اطلاعات صنعت کارت و پرداخت را دربر می‌گیرد. در این کتاب، توضیح خواهیم داد که وقتی یک تراکنش را به صورت آنلاین یا در فروشگاه انجام می‌دهید، در پشت پرده چه اتفاقی می‌افتد و چه می‌شود که در نهایت، آن تراکنش، روی صورت حساب کارت پرداخت شما ظاهر می‌شود. ما نگاهی خواهیم داشت بر پیام‌هایی که بین تمامی اعضای سیستم پرداخت رد و بدل می‌شود و سپس، بررسی خواهیم کرد که مجرمان چگونه می‌توانند در این پیام‌ها دست ببرند، آنها را سرقت و آن را به پول تبدیل کنند.

از مهم‌ترین موضوعاتی که به آنها خواهیم پرداخت، عبارت‌اند از: کدام داده‌های کارت و پرداخت در سراسر جهان به گردش در می‌آیند؟ علت وجود این همه تفاوت در استانداردهای صنعت کارت و پرداخت چیست؟ چه کسی به تطبیق هویت شما با هویت ثبت شده‌تان اهمیت می‌دهد؟ از چه متر و معیاری برای اعتبارسنجی تطبیق شما استفاده می‌شود و چگونه می‌توانیم به یک متخصص صنعت کارت و پرداخت تبدیل شویم؟

در پایان کتاب، شما درک خواهید کرد که استانداردهای صنعت کارت و پرداخت چگونه طراحی شده‌اند تا داده‌های کارت پرداختی را از دست مجرمان در امان نگه دارند. مطالعه این کتاب به هیچ پیش‌نیازی احتیاج ندارد. کتاب حاضر به شما کمک خواهد کرد تا از این به بعد، با اعتماد به نفس بالاتری روی پروژه‌های مربوط به صنعت کارت و پرداخت به فعالیت بپردازید.

تقدیم به تمام متخصصان نرم‌افزار



بخش اول
درک اینکه کارت و پرداخت
چگونه کار می کند



۱. چگونگی عملکرد تراکنش‌های پرداخت

چگونه تراکنش‌های پرداخت با کارت در صورت حساب بانکی ظاهر می‌شوند



Card Statement	
4687 38** **** 7980	
Pizza	\$13.20
Rail fare	\$56.87
Wired Brain	\$ 5.10
Coffee	
Plu	\$29.99
Web hosting	\$ 9.99
Total	\$115.15

شکل ۱-۱

آیا تاکنون برایتان سؤال پیش آمده که وقتی با استفاده از کارت‌تان، یک تراکنش، مانند خرید یک فنجان قهوه را انجام می‌دهید، چه اتفاقی می‌افتد که چند روز بعد، این تراکنش در صورت حساب بانکی یا کارتی شما نقش می‌بندد؟ بیایید با هم نحوه کار را مرور کنیم.



«لطفاً به من یک
لانه بزرگ بدهید.»



«قیمت آن ۵
دلار می‌شود.»



«من با کارت
پرداخت
خواهم کرد...»



«بفرمایید.»

شکل ۱-۲

تصور کنید «ملیندا» که دارنده کارت است، به کافی‌شاپ محبوبش، یعنی

«استارباکس» می رود و تقاضای یک لاته می کند. سوزان که یکی از دستیاران کافی شاپ است، از او می خواهد در ازای دریافت لاته، ۵ دلار بپردازد. ملیندا تصمیم می گیرد پرداختش را با کارت انجام دهد. در این قسمت، چند راهکار وجود دارد؛ ملیندا بخش نوار مغناطیسی کارت را در دستگاه می کشد، یا از طریق تماس تراشه هوشمند، کارت را درون دستگاه کارتخوان قرار می دهد و در نهایت، یک لاته خوشمزه از سوزان تحویل می گیرد.

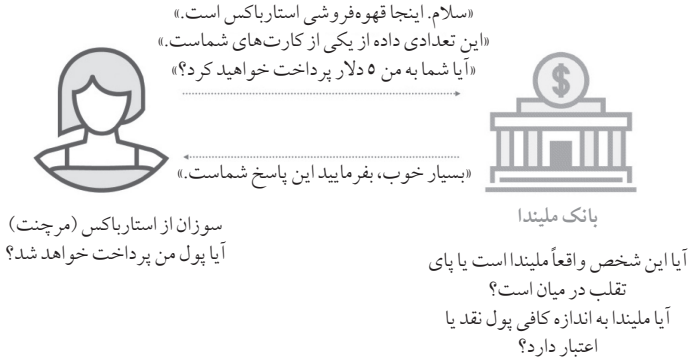
افراد به چه چیزی فکر می کنند؟



شکل ۱-۳

زمانی که ملیندا از کارتش استفاده می کند، هر یک از شرکت کنندگان در تراکنش به چه موضوعی فکر می کنند؟ سوزان از این موضوع نگران است که اگر ملیندا لاته را بگیرد و از فروشگاه بیرون برود، آیا استارباکس پولش را دریافت خواهد کرد یا خیر؟ ملیندا واقعاً دلش می خواهد لاته را بگیرد، ولی پول نقد با خودش نیاورده است، پس فقط امیدوار است که تراکنش درست عمل کند. بانک ملیندا به دنبال این است که متوجه شود آیا واقعاً خود ملیندا در حال انجام تراکنش است یا فرد دیگری خودش را به جای او جا زده است. یکی دیگر از مواردی که بانک ملیندا به آن توجه می کند، این است که آیا ملیندا پول کافی در حسابش دارد یا به اندازه ای اعتبار دارد که از پس پرداخت ۵ دلار بر بیاید؟

هدف از تأیید هویت



شکل ۴-۱

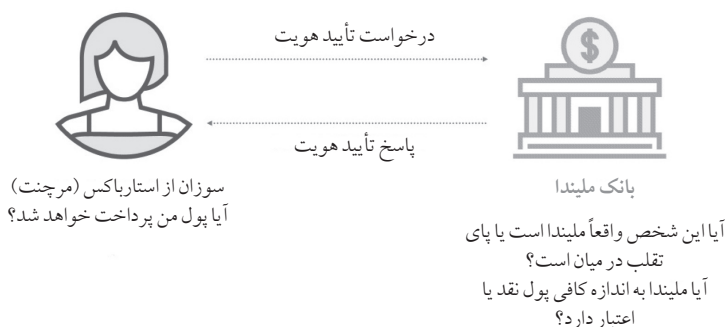
اولین گام در پردازش پرداخت، تأیید هویت است. با برداشتن این گام، پاسخ سوزان و بانک داده می شود. در حال حاضر، کسب و کارهایی که کارت های پرداختی را می پذیرند، با نام «مرچنت» شناخته می شوند. در واقع می توان گفت سوزان که نقش مرچنت را بر عهده دارد، یک پیام الکترونیکی به بانک ارسال می کند. این پیام شامل داده هایی از کارت ملیندا است و این پرسش را از بانک مطرح می کند که اگر سوزان به ملیندا اجازه بدهد که با یک لاته در دست، از کافی شاپ استارباکس خارج شود، آیا بانک مبلغ ۵,۱۰ دلار را به این کافی شاپ پرداخت خواهد کرد یا خیر؟ بانک بر اساس اطلاعاتی که از مرچنت دریافت می کند، دو موضوع را بررسی می کند. اول اینکه آیا فرد انجام دهنده تراکنش، واقعاً خود ملیندا است یا فرد دیگری خودش را به جای او گذاشته و نقش ملیندا را بازی می کند؟ بدین منظور، بانک بررسی می کند که آیا گزارشی در مورد سرقت یا مفقود شدن کارت مورد نظر به ثبت رسیده یا خیر.

احتمال دارد بانک بررسی های دیگری نیز انجام بدهد؛ برای مثال کنترل کند که آیا ملیندا در همان کشوری ساکن است که مرچنت در آنجا قرار دارد یا خیر؟ یا آیا ملیندا پیش تر از آن کافی شاپ قهوه خریده است یا خیر؟ بانک همچنین بررسی می کند که

درک اینکه کارت و پرداخت چگونه کار می کند ۱۹

سقف اعتبار ملیندا چقدر است و آیا ۵ دلار در حسابش دارد یا خیر. اگر بانک تأیید کند که آن فرد، واقعاً خود ملیندا است و او به اندازه کافی پول دارد، یک پیام را به مرچنت ارسال می کند و اعلام می کند که ملیندا می تواند لاته را تحویل بگیرد و بانک بعد از مدتی، پرداخت را به مرچنت انجام خواهد داد. این عملیات، با نام تأیید هویت (Authorization) شناخته می شود.

هدف از تأیید هویت



شکل ۵-۱

پیامی که از جانب مرچنت به بانک فرستاده می شود، با نام درخواست تأیید هویت شناخته می شود. همچنین پیامی که بانک برای مرچنت ارسال می کند، پاسخ تأیید هویت نامیده می شود.

پاسخ هایی که به درخواست تأیید هویت داده می شوند، معمولاً حاوی پیام تأیید هستند، ولی اگر بانک تصور کند که تراکنش از نوع متقلبانه است یا دارنده کارت به وجوه مالی لازم دسترسی ندارد، می تواند درخواست را رد کند. در نمونه حاضر، اگر به درخواست تأیید هویت سوزان پاسخ رد داده شود، ملیندا لاته را دریافت نخواهد کرد؛ بنابراین تأیید هویت، اولین گام در هر تراکنش پرداخت کارتی محسوب می شود. در مثال ما، ملیندا لاته اش را تحویل می گیرد و کافی شاپ استارباکس از بانک وعده می گیرد که در آینده ۵ دلار پول دریافت خواهد کرد.

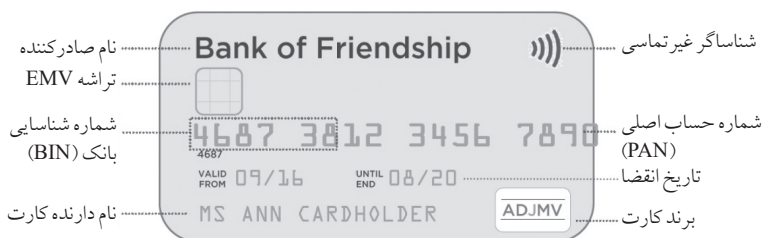
گام‌های هر تراکنش



شکل ۶-۱

ما در کتاب حاضر، نگاهی خواهیم داشت به جزئیات تأیید هویت و دیگر گام‌های فرایند پرداخت؛ این گام‌ها عبارت‌اند از: تصفیه، تسویه و بازگردانی. تصفیه و تسویه، همان روشی هستند که کافی شاپ استارباکس از طریق آنها، ۵,۱۰ دلار را دریافت خواهد کرد. دو روش برای بازگردانی تراکنش وجود دارد؛ استرداد وجه (chargeback) و بازپرداخت (Refund). دلیل ما برای انجام این بررسی، آن است که در هر یک از گام‌های مذکور، مقداری داده درون سیستم، در شبکه مرچنت و در شبکه بانک، انتقال داده می‌شود و کلید حفظ امنیت پرداخت در این است که بدانیم داده را از کجا باید پیدا کنیم، چه چیزی درون داده است و چگونه باید آن را مورد حفاظت قرار داد.

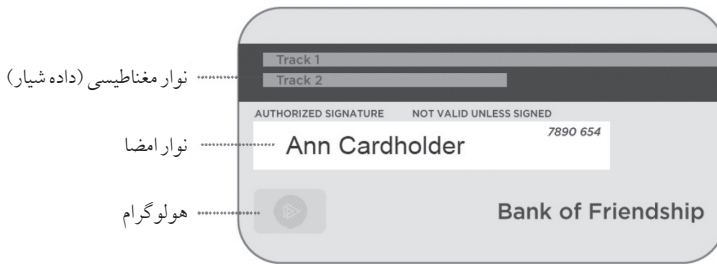
۲. داده ذخیره شده در یک کارت پرداختی



شکل ۱-۷

درست است که هر کدام از کارت‌های پرداخت از لوگوها و رنگ‌های مختلفی استفاده می‌کنند، ولی همگی آنها عناصر داده مشابهی روی خودشان دارند و در اغلب آنها، محل قرار گرفتن این عناصر روی کارت یکسان است. بنابراین بیا بید با هم بررسی کنیم که داده، کجای یک کارت قرار می‌گیرد. از قسمت بالایی شروع می‌کنیم. در این بخش، همیشه نام صادرکننده کارت که معمولاً یک بانک یا یک اسکیمای کارت (Card scheme) است، نوشته می‌شود. بعضی کارت‌ها نماد جالبی شبیه به موج روی خودشان دارند. این نماد نشان می‌دهد که کارت را می‌توان در تراکنش‌های غیرتماسی مورد استفاده قرار داد. همچنین بسیاری از کارت‌های امروزی شامل یک تراشه EMV هوشمند هستند که باعث افزایش امنیت تراکنش‌ها می‌شود، اما نوبت می‌رسد به داده‌هایی که معمولاً به شکل برجسته روی کارت نوشته می‌شوند. در بخش میانی کارت، یک شماره کارت ۱۵ یا ۱۶ رقمی وجود دارد. این عدد ۱۵ یا ۱۶ رقمی، در صنعت پرداخت با نام شماره حساب اصلی یا PAN شناخته می‌شود. شش رقم اول شماره حساب اصلی، ویژه و خاص هستند. این ارقام برای هر بانک، منحصر به فرد هستند و با نام شماره شناسایی بانک یا همان BIN شناخته می‌شوند. تمامی کارت‌ها، تاریخ

انقضا دارند و بعد از آن زمان، از درجه اعتبار ساقط می شوند؛ در برخی کارت ها عبارت «دارای اعتبار از» یا «تاریخ صدور» حک می شود. همچنین نام دارنده کارت روی کارت نوشته می شود؛ در نهایت، نوبت به یک لوگو از برند کارت می رسد. از جمله این برندها می توانیم به آمریکن اکسپرس، دیسکاور، جی سی بی، مستر کارت یا ویزا اشاره کنیم.



شکل ۸-۱

بیاید کارت را برگردانیم. در قسمت پشتی کارت، اطلاعات کمتری نسبت به بخش رویی آن وجود دارد. نوار مغناطیسی شامل تمام داده هایی است که روی کارت نوشته شده است. این نوار داده های بیشتر دیگری را هم در خودش جای داده است. تمام این داده ها به شکل دیجیتال هستند و مرچنت با کمک تجهیزاتی می تواند آنها را بخواند. در واقع، نوار مذکور شامل دو شیار داده مختلف است که ترک (Track) نامیده می شوند و توسط سیستم مرچنت ها، قابل خواندن هستند. این دو شیار با اسامی ترک ۱ و ترک ۲ روی کارت دیده می شوند. اغلب نوارهای مغناطیسی به رنگ سیاه یا قهوه ای پررنگ هستند، ولی برخی تولیدکنندگان به سختی تلاش کرده اند تا نوارهای مغناطیسی را در رنگ های جذاب نقره ای یا طلایی بسازند؛ بنابراین ممکن است نوارهای مغناطیسی بیشتر شبیه به یک تزئین دیده شوند، نه یک بخش کاربردی؛ ولی به هر شکل، همیشه وجود خواهند داشت و از نظر فیزیکی، در همان بخش بالایی کارت تعبیه خواهند شد. دلیل وجود نوار مغناطیسی این است که وقتی دارنده کارت یک رسید را امضا می کند، مرچنت بتواند امضای روی رسید را با امضایی که روی کارت وجود دارد، مقایسه کند. بله می دانم، مرچنت ها، دیگر امضاها را به شکل فیزیکی کنترل نمی کنند، ولی به هر روی،

در این قسمت، مقداری داده نیز وجود دارد که در فرایند احراز هویت به کار گرفته می‌شود تا ثابت شود کارت واقعی است. این داده‌ها، داده حساس احراز هویت (SAD) نامیده می‌شوند. مرچنت، این داده‌ها را به صادرکننده ارسال می‌کند تا بگوید اگر من به این داده دسترسی دارم، احتمال اینکه کارت واقعی را دریافت کرده باشم، از احتمال جعلی بودن آن بیشتر است. روی ترک ۱، دو نوع داده حساس احراز هویت را می‌توان پیدا کرد. نوع اول، یک عدد سهرقمی محرمانه است که در هیچ قسمتی از کارت چاپ نشده و فقط بانک صادرکننده از آن اطلاع دارد. هر برند کارت، نام متفاوتی برای این عدد انتخاب کرده و این موضوع، گاهی اوقات سردرگم‌کننده می‌شود. ویزا عدد سهرقمی مذکور را ارزش تایید کارت یا CVV می‌نامد، مسترکارت نیز نام کد تأیید کارت یا CVC را برای این عدد انتخاب کرده است. هر دو نام، رایج هستند و در مراجع مختلف، به هر دو اشاره شده است، ولی من در بیشتر بخش‌های کتاب، اصطلاح CVV را مورد استفاده قرار خواهم داد. در نوار مغناطیسی، یک ارزش دیگر نیز گنجانده شده که ارزش تأیید پین یا PVV نامیده می‌شود و با هدف صحت‌سنجی پین‌ها مورد استفاده قرار می‌گیرد. من در شکل فوق، چیزهایی که ممکن است بعد از ارزش تایید کارت وجود داشته باشد را نشان نداده‌ام. اساساً، قانون به این شکل است که صادرکننده کارت می‌تواند اقدامات دلخواهش را روی داده‌هایی که پس از ارزش تایید کارت قرار می‌گیرند، انجام بدهد. در این قسمت CVV و PVV نوشته می‌شود. پرداختن به این موضوع اهمیت دارد؛ زیرا در برخی قوانین استاندارد امنیت داده صنعت کارت و پرداخت، مشخص شده که مرچنت کدام داده‌ها را می‌تواند ذخیره کند و کدام بخش از داده‌ها را مجاز نیست ذخیره‌سازی کند.

[illegible]

شما می‌توانید این قسمت را تا
کد سرویس، ذخیره‌سازی کنید.

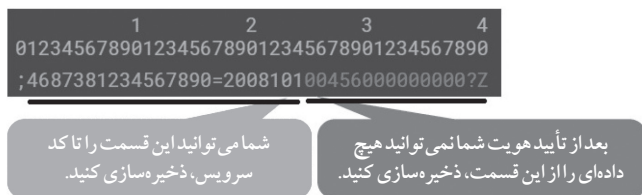
بعد از تأیید هویت شما نمی توانید هیچ داده‌ای را از این قسمت، ذخیره‌سازی کنید.

اساساً مرچنت هر زمان که بخواهد، می تواند اطلاعات بخش سیاه رنگ را تقسیم کند
 سرویس، ذخیره کند. در ادامه کتاب، توضیح خواهیم داد که چرا مرچنت داده های مذکور
 را ذخیره می کند و در کل، ذخیره کردن این داده ها فکر خوبی هست یا نه. داده هایی که
 در سمت راست کد سرویس هستند و بارنگ مشکی زیرشان خط کشیده شده است،
 توسط صادرکننده تعیین می شوند و من آنها را با تعداد زیادی صفر نشان داده ام. مرچنت
 نمی تواند بعد از تأیید هویت، داده های سمت راست کد سرویس را ذخیره کند.



شکل ۱-۱۲

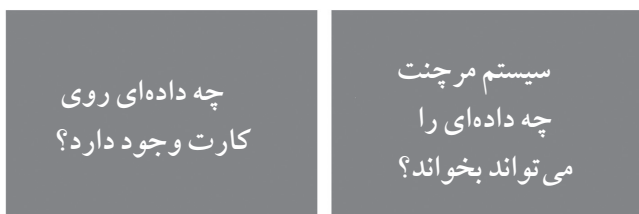
اگر به شیار بعدی، یعنی ترک ۲ نگاه کنیم، مشاهده می‌کنیم که در مقایسه با ترک ۱ بسیار کوتاه‌تر است. ترک ۲ تنها از ۴۰ کاراکتر تشکیل شده است. در ترک ۲ نیز مشابه ترک ۱ شماره حساب اصلی، تاریخ انقضا و کد سرویس به چشم می‌خورد. یکی دیگر از وجوه شباهت ترک ۲ با ترک ۱ در این است که هر چه به قسمت سمت راست کد سرویس حرکت کنیم، به اطلاعاتی نزدیک می‌شویم که صادرکننده کارت قادر است از آنها استفاده کند.



شکل ۱-۱۳

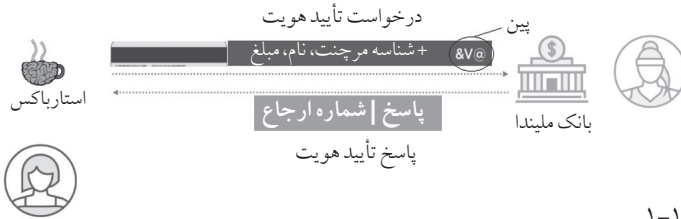
درست همانند قسمت قبل، شما نمی توانید بعد از تأیید هویت، داده‌ای را از قسمت سمت راست کد سرویس، ذخیره‌سازی کنید. معمولاً CVV یا همان ارزش تأیید کارت در این قسمت نوشته می‌شود.

۳. نهادهای دست اندر کار در اعطای اجازه قانونی به یک تراکنش پرداخت با کارت



شکل ۱۴-۱

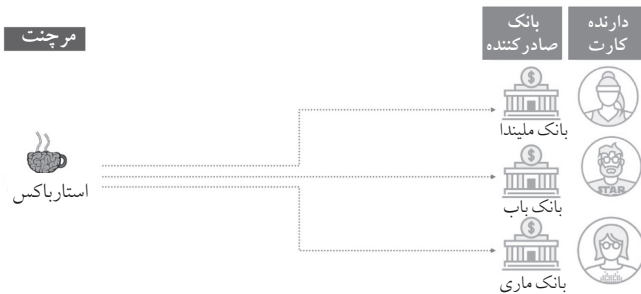
به خاطر داشته باشید که هدف از تأیید هویت، خواندن داده از روی کارت مشتری و ارسال آن به بانک صادرکننده است. نحوه خواندن داده از کارت، به این بستگی دارد که شما در کدام قسمت از دنیا قرار دارید. شیوه ذخیره‌سازی داده روی کارت، تاریخ دسترسی به داده و قابلیت‌های فنی مرچنت همگی روی نحوه خواندن داده از کارت نقش دارند. سه روش وجود دارد که مرچنت‌ها از طریق آنها می‌توانند تراکنش را بپذیرند. اگر تراکنش از نوع نوار مغناطیسی باشد، مرچنت می‌تواند به وسیله یک دستگاه پرداخت یا یک کارت خوان اختصاصی، کارت را در دستگاه پایانه فروش بکشد. در روش EMV یا تراشه، مرچنت، کارت را درون یک دستگاه سازگار با EMV وارد می‌کند. در تراکنش‌های غیرتماسی نیز دارنده کارت، به سادگی کارت را نزدیک دستگاه کارت خوان می‌گیرد. در هر سه نوع مختلف تراکنش، اطلاعات از کارت خوانده می‌شود و وارد سیستم‌های مرچنت می‌شود. در مرحله بعدی، اطلاعات خوانده‌شده برای درخواست تأیید هویت به کار گرفته می‌شوند. بیایید بحث را با بررسی تراکنش نوع اول، یعنی نوار مغناطیسی شروع کنیم. در بخش بعدی، تراکنش‌های تراشه یا EMV را نیز زیر ذره‌بین خواهیم برد.



شکل ۱-۱۵

تجهیزات مرچنت، تمام داده‌های ترک ۱ را از روی کارت می‌خواند و این داده‌ها را در کنار اطلاعاتی از مرچنت و مبلغ تراکنش به بانک صادرکننده می‌فرستد. امکان دارد یک ارزش رمزگذاری شده مبتنی بر پین نیز به بانک ارسال شود. این فرایند، درخواست تأیید هویت نام دارد. بانک صادرکننده کارت، داده‌ها را مورد بررسی قرار می‌دهد، تعیین می‌کند که آیا تراکنش واقعی است یا تقلبی و سپس، کنترل می‌کند که آیا وجه یا اعتبار کافی برای انجام تراکنش وجود دارد یا خیر. بعد از انجام تمامی این بررسی‌ها، بانک، پاسخ تأیید هویت را به مرچنت می‌فرستد. این پاسخ، دربرگیرنده عبارت قبول یارد و یک شماره یا کد ارجاع است تا مشخص شود که مرچنت، پاسخ درخواستش را دریافت کرده است.

تأیید هویت در عمل

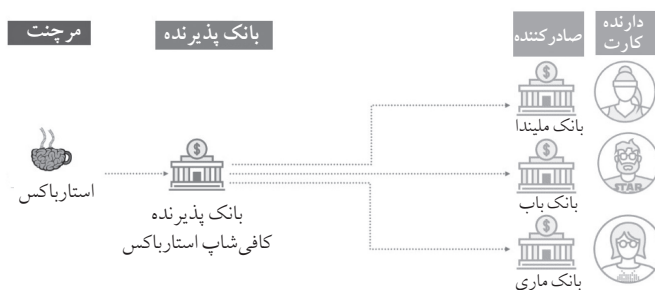


شکل ۱-۱۶

حال برای اینکه چنین روندی اتفاق بیفتد، کافی شاپ استارباکس که نقش مرچنت

را بر عهده دارد، باید با تمامی بانک‌های جهان که کارت پرداختی صادر کرده‌اند، وارد ارتباط شود تا در صورتی که یکی از مشتریان آن بانک وارد کافی شاپ شود، بتواند به او سرویس ارائه دهد. این تعداد ارتباط، برای یک مرچنت، بسیار زیاد است.

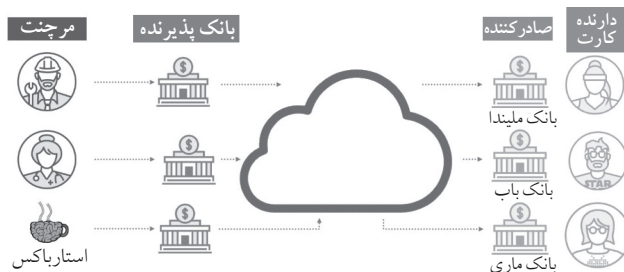
تأیید هویت در عمل



شکل ۱۷-۱

چیزی که در عمل اتفاق می‌افتد، این است که هر مرچنت که کارت‌های پرداخت را قبول می‌کند، با یک بانک پذیرنده وارد ارتباط می‌شود. نوعی بانک است که تراکنش‌های با کارت مرچنت‌ها را دریافت می‌کند و با تمامی بانک‌های جهان که کارت صادر کرده‌اند، ارتباط برقرار می‌کند.

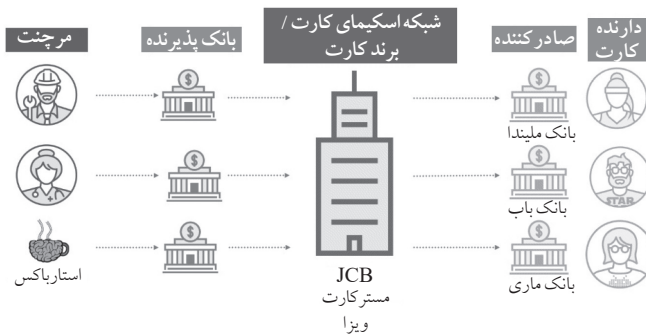
تأیید هویت در عمل



شکل ۱۸-۱

البته این عملیات به شدت پیچیده است. صدها بانک پذیرنده وجود دارد و اگر هر کدام از آنها بخواهند با تمامی بانک‌های صادرکننده کارت ارتباط بگیرند و با هر کدام قراردادهای جداگانه ببندند، به تعداد انبوهی وکیل نیاز خواهند داشت و سرانجام زیر کوهی از کاغذبازی‌ها دفن خواهند شد.

تأیید هویت در عمل

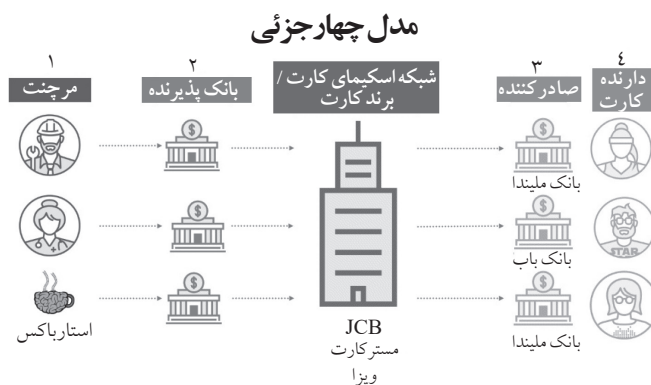


شکل ۱۹-۱

بنابراین باید یک عامل میانی وجود داشته باشد که تمامی بانک‌های پذیرنده را به کل بانک‌های صادرکننده متصل کند. این عامل، شبکه‌های اسکیمای کارت یا به قول فعالان صنعت پرداخت، برندهای کارت هستند. ویزا، مسترکارت و جی‌سی‌بی نمونه‌هایی از این برندهای کارت هستند. آنها کل بانک‌های پذیرنده را به تمام بانک‌های صادرکننده کارت متصل می‌کنند. بنابراین، در مثال ما، درخواست تأیید هویت از کافی‌شاپ استارباکس به بانک پذیرنده استارباکس ارسال می‌شود و سپس به شبکه اسکیمای کارت، از قبیل ویزا یا مسترکارت فرستاده می‌شود. در مرحله بعدی، شبکه اسکیمای کارت، درخواست تأیید هویت را به بانک صادرکننده ملیندا ارسال می‌کند و منتظر دریافت پاسخ تأیید هویت از جانب بانکی که کارت ملیندا را صادر کرده، می‌ماند.

وقتی بانک پاسخ را اعلام کرد، شبکه اسکیمای کارت نتیجه را به بانک پذیرنده استارباکس می‌فرستند. اکنون، وقت آن رسیده که با یکی از مهم‌ترین موضوعات در مورد صنعت پرداخت آشنا شویم. درست است که این صنعت پر از استانداردها و قوانین است، ولی از آنجایی که کل جهان را شامل می‌شود، تفاوت‌های زیادی در نحوه کار سیستم‌ها دیده می‌شود.

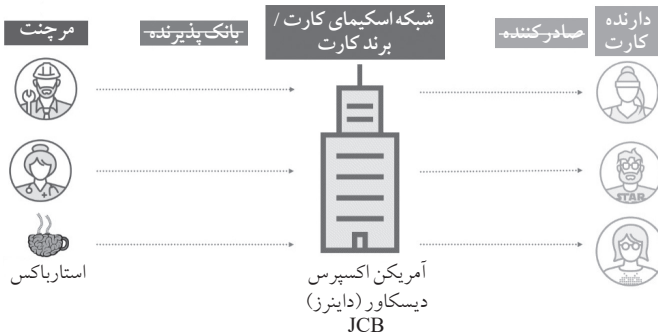
کشوری که در آن ساکن هستید، قوانین محلی و تاریخیچه نحوه انجام پرداخت‌ها در یک منطقه خاص و بسیاری از دلایل مختلف، در شکل‌گیری این تفاوت‌ها نقش دارند. بنابراین، اگرچه اصول کلی این عملیات همیشه معتبر است، ولی همیشه در محل‌های گوناگون، تفاوت‌هایی را پیدا خواهید کرد. هیچ روش جهانی واحدی برای انجام پرداخت وجود ندارد و این امر، همان چیزی است که کار کردن در صنعت پرداخت را به امری جذاب تبدیل کرده است.



شکل ۲۰-۱

اولین مورد خلاف قاعده ما این است که همه پرداخت‌های کارتی، به شیوه‌ای که در شکل نشان دادیم، یعنی مدل چهار جزئی مرچنت، بانک پذیرنده، صادرکننده و دارنده کارت، انجام نمی‌شوند. یک روش دیگر به نام مدل سه جزئی نیز وجود دارد که اغلب پرداخت‌ها به آن شیوه صورت می‌گیرند.

مدل سه جزئی



شکل ۲۱-۱

در مدل سه جزئی، خبری از بانک پذیرنده یا بانک صادرکننده نیست. شبکه اسکیمای کارت، به شکل مستقیم، کارت را به دارنده کارت می دهد و به صورت مستقیم، با مرچنت ها وارد ارتباط می شود تا تراکنش های آنها را بپذیرد. آمریکن اکسپرس و دیسکاور، دو نمونه شبکه اسکیمای کارت هستند که اساساً یک شبکه اسکیمای شخص ثالث به شمار می روند. در برخی مناطق جهان، دیسکاور را با نام «داینرز» نیز می شناسند. لازم به ذکر است جی سی بی، هم در مدل سه جزئی و هم در مدل چهار جزئی کار می کند. به هر روی، چه از شبکه اسکیمای سه جزئی استفاده شود و چه چهار جزئی، در پایان فرایند تأیید هویت، مرچنت یک وعده برای پرداخت از بانک دارنده کارت (یا در شبکه اسکیمای سه جزئی: از صادرکننده کارت) دریافت می کند و دارنده کارت، به قهوه اش می رسد. گام بعدی، آشنایی با روش دریافت پول واقعی توسط مرچنت است.

۴. دریافت پول؛ تصفیه و تسویه

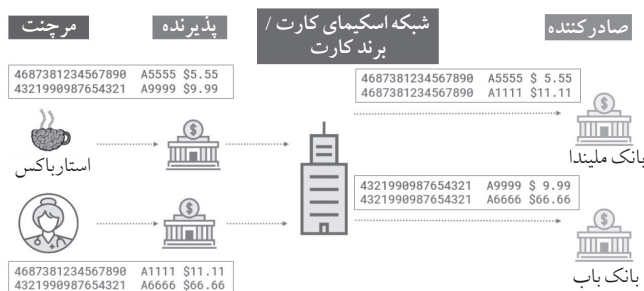
دریافت پول؛ تصفیه و تسویه



شکل ۲۲-۱

مراحل از فرایند پرداخت که طی آنها، پول به مرچنت پرداخت می‌شود، تصفیه و تسویه نامیده می‌شوند.

تصفیه (چهار جزئی)

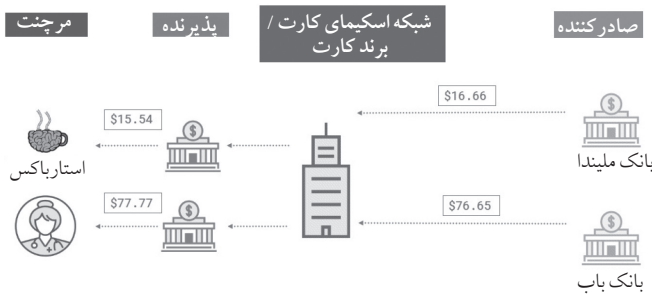


شکل ۲۳-۱

در مرحله تصفیه، هر مرچنت خلاصه‌ای از تمام تراکنش‌های روزش را به بانک پذیرنده ارسال می‌کند. این داده‌ها، عموماً شامل شماره حساب اصلی کارت مورد استفاده

برای انجام تراکنش، شماره ارجاع تأیید هویت و مبلغ می شود. هیچ کدام از داده های مورد استفاده برای تأیید هویت، از جمله داده های شیارها، در پیام تصفیه وارد نمی شوند. بنابراین بهتر است توجه داشته باشیم که پیام های تأیید هویت، در مقایسه با پیام های تصفیه، داده های بیشتری را شامل می شوند. در گام بعدی، هر بانک پذیرنده، تراکنش های مربوط به هر مرجنت را بخش بندی می کند و به شبکه اسکیمای کارت مربوطه می فرستد. من در شکل، برای سادگی بیشتر، تنها یک شبکه اسکیمای کارت را به تصویر کشیده ام. شبکه اسکیمای کارت، براساس شش رقم ابتدایی شماره حساب اصلی، بررسی می کند که هر تراکنش مربوط به کدام بانک صادرکننده است. اگر به خاطر داشته باشید، این عدد شش رقمی، همان شماره شناسایی بانک است. در گام بعدی، بانک پذیرنده تمامی تراکنش ها را به بانک صادرکننده مربوط به هر کدام می فرستد.

تسویه (چهار جزئی)

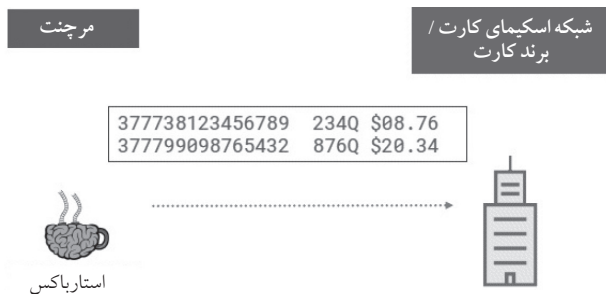


شکل ۲۴-۱

بانک صادرکننده بررسی می کند که به ازای هر تراکنش موجود در داده های تصفیه روزانه، چه مقدار به شبکه اسکیمای کارت مقروض است و سپس، مبلغ را به این شبکه ارسال می کند. به این فرایند، تسویه گفته می شود. سپس، شبکه اسکیمای کارت مبالغ دریافتی را به بانک های پذیرنده انتقال می دهد؛ بانک پذیرنده نیز مبالغ را از هم تفکیک کرده و برای مرجنت ها می فرستد. برخی مرجنت ها، روز بعد از انجام تراکنش،

وجوه‌شان را دریافت می‌کنند، اما بعضی دیگر ممکن است چند روز یا حتی یک ماه برای دریافت پول‌شان منتظر بمانند. فاصله زمانی بین انجام تراکش و واریز وجه به حساب مرچنت، بر اساس توافق بین مرچنت و بانک پذیرنده تعیین می‌شود و عمدتاً به نوع کالاها یا خدمات مرچنت و مدت زمان انجام کسب و کار توسط مرچنت بستگی دارد.

تصفیه (سه جزئی)



شکل ۱-۲۵

اکنون به تصفیه در شبکه اسکیمای سه جزئی می‌رسیم. به خاطر داشته باشید که در مدل سه جزئی، نقش بانک پذیرنده و بانک صادرکننده حذف می‌شود؛ بنابراین، مرچنت خلاصه‌ای از تمامی تراکش‌های روزانه‌اش را به شکل مستقیم، به شبکه اسکیمای کارت ارسال می‌کند.

تسویه (سه جزئی)



شکل ۱-۲۶

در مرحله بعد، شبکه اسکیمای کارت عملیات تسویه را انجام داده و وجه تمامی تراکنش‌ها را به مرچنت انتقال می‌دهد.

موارد خلاف قاعده

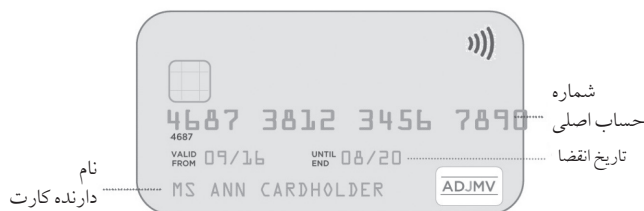
این گونه نیست که در تمامی تراکنش‌ها، فرایند تأیید هویت طی شود.	این احتمال وجود دارد که مرچنت‌ها، پرونده‌های تصفیه را ارسال نکنند.	برخی مرچنت‌ها، پرونده‌های تصفیه‌شان را «پرونده‌های تسویه» می‌نامند.
قالب‌های پیام بین بانک‌های پذیرنده، شبکه‌های اسکیمای کارت و کشورهای مختلف، با هم تفاوت دارد.	در برخی کشورها، فرایند تصفیه وجود ندارد.	

شکل ۲۷-۱

گفتیم در سیستم پرداخت، موارد خلاف قاعده رخ می‌دهد؟ این عملکرد خلاف قاعده در تأیید هویت، تصفیه و تسویه، بسیار پررنگ است. اول از همه، بهتر است بدانید همیشه این گونه نیست که در تمام تراکنش‌ها، فرایند تأیید هویت طی شود. بسته به مبلغ تراکنش و روش انجام تراکنش، گاهی اوقات ممکن است درخواست تأیید هویت ارسال نشود. بعضی اوقات، مرچنت بعد از آنکه داده دارنده کارت را ثبت می‌کند، تصمیم می‌گیرد اعتماد کند که مبلغ را دریافت خواهد کرد. اغلب مواقع، مرچنت پرونده تصفیه را ارسال نمی‌کند و بانک پذیرنده یا شبکه اسکیمای کارت، این کار را برای آنها انجام می‌دهد. بعضی اوقات نیز مرچنت پرونده تصفیه را تهیه می‌کند، ولی نام آن را پرونده تسویه می‌گذارد. قالب‌های پیام و محتوای پیام‌های ارسال شده بین بانک‌های پذیرنده، مرچنت‌ها و شبکه‌های اسکیمای کارت، در بانک‌های پذیرنده کشورهای گوناگون و شبکه‌های اسکیمای پرداخت مختلف، با هم تفاوت دارد. در گروهی از کشورها، فرایند تصفیه وجود ندارد و تسویه، همواره از طریق درخواست تأیید هویت انجام می‌گیرد. اما هر اتفاقی هم که بیفتد، همواره دست کم یک پیام وجود خواهد داشت که از سوی مرچنت به صادرکننده ارسال می‌شود و در پی ارسال این پیام، مبلغ از حساب دارنده کارت برداشت شده و به مرچنت انتقال داده می‌شود.

۵. تراکنش‌های تجارت الکترونیکی و ارائه‌دهندگان خدمات پرداخت (PSP)

در یک تراکنش تجارت الکترونیکی که ممکن است شما آن را با نام تراکنش بدون حضور کارت یا تراکنش سی‌ان‌پی (CNP) بشناسید، به شکل مشابه، همین گام‌های تأیید هویت، تصفیه و تسویه طی می‌شوند؛ بنابراین بیا باید تصور کنیم که دارنده کارت ما، یعنی ملیندا، قصد دارد با استفاده از کارت خودش، مقداری دانه قهوه از وب‌سایت استارباکس خریداری کند.



شکل ۲۸-۱

اطلاعات مورد نیاز ملیندا، روی کارت او چاپ شده است. از جمله این اطلاعات می‌توانیم به شماره حساب اصلی، تاریخ انقضا و نام او اشاره کنیم که روی کارت به چاپ رسیده‌اند.



شکل ۲۹-۱

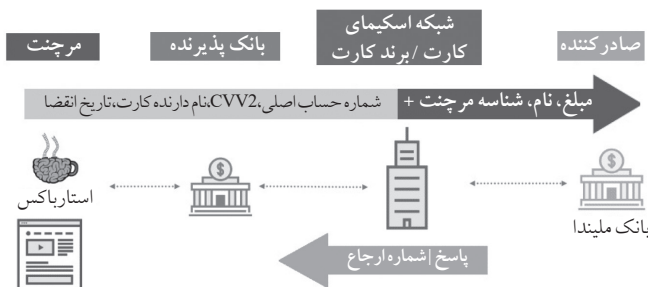
پشت کارت، یک کد امنیتی چاپ شده است. این کد نیز مانند کد امنیتی رمزگذاری شده در نوار مغناطیسی، در شبکه‌های مختلف اسکیمای کارت، با نام‌های متفاوتی شناخته می‌شود. در حالت کلی، من این کد را ارزش تأیید کارت ۲ یا CVV2 می‌نامم. ویزا نیز این کد را با نام CVV2 می‌شناسد، ولی مسترکارت نام CVC2 را برای آن انتخاب کرده است. مهم است بدانیم این عدد سه‌رقمی، با عدد CVV که در نوار مغناطیسی رمزگذاری شده است، تفاوت دارد. به این ترتیب، اگر یک مجرم داده‌ها را از وب‌سایت به سرقت ببرد، به عدد CVV ثبت‌شده در نوار مغناطیسی دسترسی نخواهد داشت و فقط از عدد CVV2 اطلاع خواهد داشت؛ در نتیجه قادر به کپی کردن کارت نخواهند بود.

به شکل مشابه، اگر یک مجرم داده‌ها را از یک سیستم پایانه فروش سرقت کند، از داده مربوط به CVV2 بی‌اطلاع خواهد بود و نخواهد توانست از طریق آن کارت، خرید اینترنتی انجام دهد. ویزا، مسترکارت، دیسکاور و جی‌سی‌بی، همگی یک کد امنیتی سه‌رقمی را روی نوار مغناطیسی در بخش پشتی کارت چاپ می‌کنند. آمریکن اکسپرس نیز یک کد امنیتی چهاررقمی دارد که آن را CID نامیده و در قسمت جلویی کارت «امکس» به چاپ رسانده است. CID در سمت راست، یا زیر شماره حساب اصلی، نوشته می‌شود.

مراحل یک تراکنش الکترونیکی، مشابه مراحل یک تراکنش معمولی است. این مراحل عبارت‌اند از: تأیید هویت، تصفیه و تسویه؛ اما در دنیای تجارت الکترونیکی، یک مورد خلاف قاعده بسیار دیده می‌شود. این مورد خلاف قاعده، گامی است که با نام «ثبت» شناخته می‌شود. مرحله ثبت بعد از تأیید هویت قرار دارد. بین زمان پذیرش یک تراکنش الکترونیکی توسط مرجع و تحویل کالا به مشتری، یک تأخیر وجود دارد و مرحله ثبت، به دلیل همین تأخیر به وجود آمده است. لازم به ذکر است همیشه روال این گونه نیست که در تمامی فرایندهای تجارت الکترونیکی، حتماً مرحله ثبت طی شود.

طی کردن یا نکردن این مرحله، به نحوه همکاری بانک پذیرنده با مرجع و نوع فعالیت مرجع بستگی دارد.

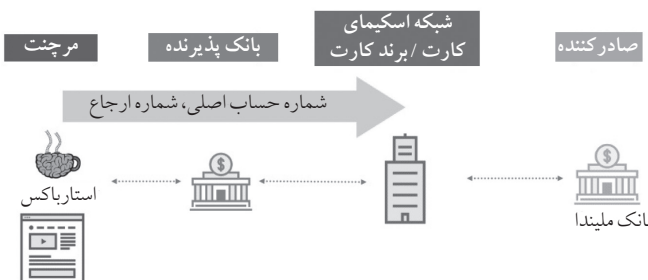
تأیید هویت در تجارت الکترونیکی



شکل ۳۰-۱

بیاپید با هم نگاهی داشته باشیم بر فرایند تأیید هویت در تجارت الکترونیکی. در یک فرایند معمول تأیید هویت برای انجام تجارت الکترونیکی، دارنده کارت، داده‌هایش را در وب‌سایت مرچنت وارد می‌کند. این داده‌ها، شامل شماره حساب اصلی کارت، CVV2، نام دارنده کارت و تاریخ انقضا هستند. به منظور تأیید هویت، داده‌های مذکور، به همراه جزئیات مرچنت و مبلغ تراکنش، به بانک صادرکننده ارسال می‌شوند. در فرایند تأیید هویت برای تجارت الکترونیکی نیز درست مثل تراکنش حضوری، مرچنت یک پیام حاوی پاسخ برای تأیید هویت از جانب بانک صادرکننده دریافت می‌کند.

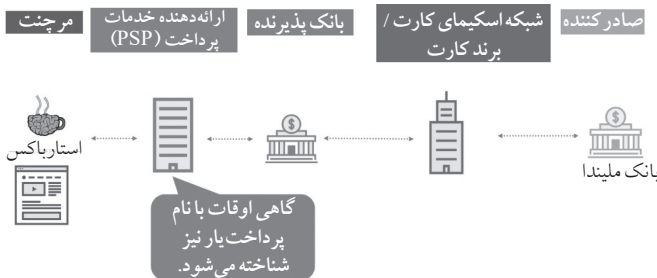
ثبت تجارت الکترونیکی



شکل ۳۱-۱

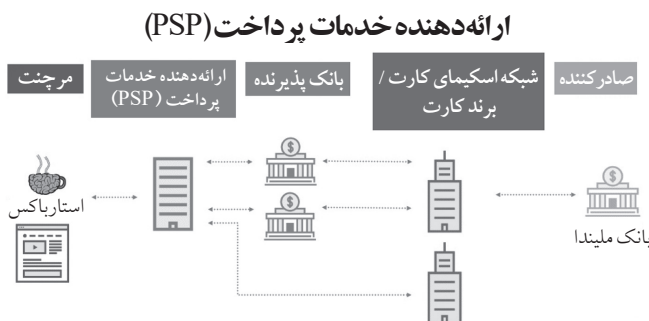
در برخی موارد، بین زمانی که مشتری کالا یا خدمات را سفارش می‌دهد و زمانی که مرچنت آنها را برای مشتری ارسال می‌کند، یک تأخیر ایجاد می‌شود. به عنوان یک نکته، به خاطر داشته باشید این گونه نیست که در تمامی تراکنش‌های تجارت الکترونیکی، تأخیر وجود داشته باشد. در صورت وجود تأخیر، مرچنت بعد از انجام سفارش توسط مشتری، ترتیبی می‌دهد که در کنار ارسال درخواست تأیید هویت، درخواست ثبت را نیز به بانک پذیرنده ارسال کند تا تأیید شود که تراکنش به شکل واقعی در حال انجام است و مرچنت به وظایفی که در قرارداد دارد، عمل می‌کند. تراکنش ثبت، عموماً شامل شماره حساب اصلی و یک شماره ارجاع است.

ارائه‌دهنده خدمات پرداخت (PSP)



شکل ۳۲-۱

در اغلب تراکنش‌های تجارت الکترونیکی، یک شخص ثالث دیگر نیز وجود دارد که بین مرچنت و بانک پذیرنده قرار می‌گیرد. این شخص ثالث، ارائه‌دهنده خدمات پرداخت یا پی‌اس‌پی نامیده می‌شود. همه مرچنت‌ها، فارغ از اندازه و مقیاس کاری‌شان، می‌توانند از سرویس ارائه‌دهندگان خدمات پرداخت استفاده کنند. در دوران ابتدایی ظهور تجارت الکترونیکی، ارائه‌دهندگان خدمت پرداخت کسانی بودند که روی چگونگی انجام پرداخت‌های کارتی در بستر اینترنت کار می‌کردند. امروزه، ارائه‌دهندگان خدمت پرداخت با نام پرداخت یاران نیز شناخته می‌شوند.



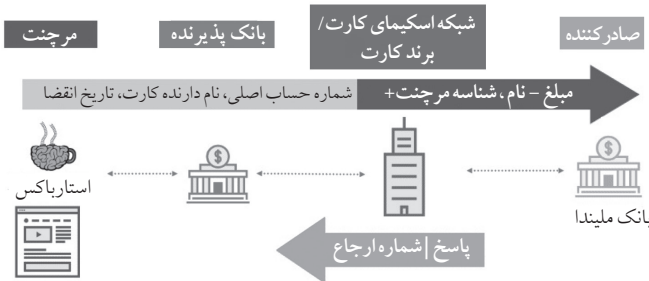
شکل ۳۳-۱

یک ارائه‌دهنده خدمات پرداخت، مسئولیت تمامی کاغذبازی‌های پیچیده بانک‌های پذیرنده و شبکه‌های اسکیمای کارت را بر عهده می‌گیرد و بدین ترتیب، به مرچنت‌های کوچک کمک می‌کند تا به راحتی، شروع به فروش در بستر اینترنت کنند. ارائه‌دهندگان خدمات پرداخت برای مرچنت‌های بزرگ نیز یک موهبت به‌شمار می‌روند؛ زیرا با وجود آنها، مرچنت‌ها به جای سروکار داشتن با نهادهای مختلف، تنها با ارائه‌دهنده خدمات پرداخت ارتباط دارند و می‌توانند به ارائه‌دهنده اعلام کنند که تراکنش اولی را به یک بانک پذیرنده ارسال کند، تراکنش دومی را به یک بانک پذیرنده دیگر و تراکنش سوم را مستقیماً به شبکه اسکیمای کارت بفرستد. بنابراین، می‌توان گفت ارائه‌دهندگان خدمات پرداخت، زمینه را فراهم می‌کنند تا مرچنت‌ها بتوانند به صورت مستقل از بانک‌های پذیرنده، به فعالیت بپردازند. در نتیجه، کار مرچنت‌ها برای مذاکره با بانک‌های پذیرنده در مورد نرخ‌های انواع تراکنش‌ها یا ارزش‌های مختلف آسان می‌شود. یک ارائه‌دهنده خدمات پرداخت، می‌تواند به تمامی مرچنت‌های بزرگ و کوچک سرویس ارائه دهد. در تراکنش‌های تجارت الکترونیکی، عملیات تسویه درست به همان روش تراکنش‌های حضوری انجام می‌پذیرد. پرونده‌های تسویه از سمت مرچنت به بانک‌های پذیرنده ارسال می‌شوند، سپس بانک‌های پذیرنده آنها را به شبکه‌های اسکیمای کارت می‌فرستند، شبکه‌های اسکیمای نیز پرونده‌ها را به بانک‌های صادرکننده ارسال می‌کنند و در نهایت، پول تسویه مسیر برعکس این فرایند را طی کرده و به دست مرچنت می‌رسد.

۶. بازگردانی یک تراکنش؛ بازپرداخت و استرداد وجه

تا به اینجا، دریافتیم که مرچنت‌ها با چه روشی برای تراکنش‌ها مجوز گرفته و پول‌شان را دریافت می‌کنند. همچنین دانستیم که داده‌های مورد استفاده در پیام‌های تأیید هویت و تصفیه، همان‌هایی هستند که بانک صادرکننده از آنها استفاده می‌کند تا اطمینان حاصل کند که یک تراکنش، در صورت حساب دارنده کارت ثبت خواهد شد، اما در مواردی که اوضاع طبق انتظار پیش نرود، چه اتفاقی می‌افتد؟ اگر یک تراکنش به اشتباه از صورت حساب یک دارنده کارت دیگر سر دربی‌آورد، چه می‌شود؟ اگر نظر دارنده کارت عوض شود یا از محصول یا سرویس مرچنت ناراضی باشد و بخواهد سفارشش را پس بدهد، چه کاری باید انجام شود؟ در چنین مواقعی، لازم است که تراکنش‌های کارت بازگردانی شوند. برای بازگردانی یک تراکنش، دو روش وجود دارد.

بازپرداخت: عملیات از جانب مرچنت آغاز می‌شود



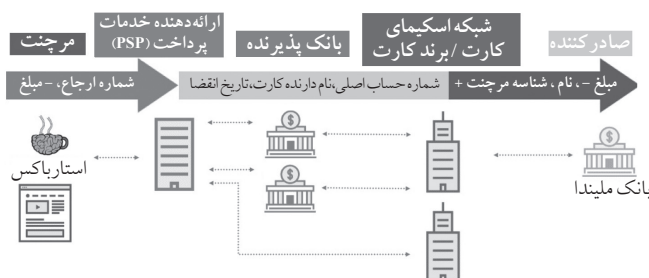
شکل ۳۴-۱

در وهله اول، شرایطی را بررسی می‌کنیم که مرچنت یک تراکنش را بازپرداخت

می‌کند. بدین منظور، مرچنت پیامی مشابه با درخواست تأیید هویت را به بانک صادرکننده کارت ارسال می‌کند. در بازگردانی، بر خلاف درخواست تأیید هویت، عموماً نیازی نیست که داده حساس تأیید هویت را داخل پیام وارد کنیم؛ صرفاً شماره حساب اصلی، نام دارنده کارت، تاریخ انقضا و مبلغ لازم برای بازگردانی به دارنده کارت، کفایت می‌کند.

همان‌گونه که انتظار می‌رود، صادرکننده در پاسخ مرچنت، یک پیام بازپرداخت به او می‌فرستد.

بازپرداخت: عملیات از جانب مرچنت آغاز می‌شود

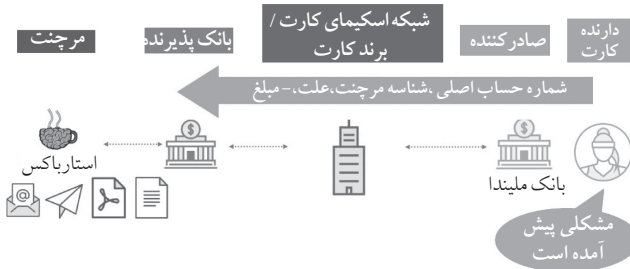


شکل ۳۵-۱

در مواردی که مرچنت از ارائه دهنده خدمات پرداخت کمک می‌گیرد، عملیات بازپرداخت آسان‌تر انجام می‌شود. در این شرایط، مرچنت تنها باید شماره ارجاع تراکنش ارائه دهنده خدمات پرداخت و مبلغ را به ارائه دهنده خدمات پرداخت ارسال کند.

در مرحله بعدی، خود ارائه دهنده پیام‌های لازم را آماده کرده و به بانک صادرکننده می‌فرستد. به خاطر داشته باشید بازپرداخت، همیشه از جانب مرچنت آغاز می‌شود.

استرداد وجه: عملیات از جانب دارنده کارت آغاز می شود



شکل ۳۶-۱

دارنده کارت نیز می تواند تراکنش را بازگردانی کند. بدین منظور، دارنده کارت باید با بانک وارد ارتباط شده و اعلام کند که تراکنش را خودش انجام نداده و پای تقبل در میان بوده است یا اینکه مرچنت به تعهداتی که در قبال دارنده کارت داشته، عمل نکرده است. این نوع از تراکنش ها را استرداد وجه نام گذاری می کنند. در گام اول، دارنده کارت با بانک صادرکننده تماس می گیرد و عنوان می کند که مشکلی پیش آمده است. در این مرحله، معمولاً لازم است که دارنده کارت یک فرم را تکمیل کند. سپس، بانک صادرکننده از طریق شبکه اسکیمای کارت، پیامی به بانک پذیرنده مرچنت می فرستد و درخواست می کند که پول بازگردانده شود. در پیام مذکور، دلیل تقاضا برای بازگشت وجه توضیح داده می شود. احتمال دارد در این پیام، یک نسخه کپی از فرمی که توسط دارنده کارت تکمیل شده نیز گنجانده شود. در این هنگام بانک پذیرنده با مرچنت تماس می گیرد و از او می خواهد اثبات کند که تراکنش، معتبر بوده است. این عملیات به روش های مختلفی انجام می شود؛ ممکن است پیام از طریق فکس یا ایمیل به دست مرچنت برسد، ولی امروزه عموماً روال به این ترتیب است که بانک پذیرنده یک وبسایت طراحی می کند و آن را در دسترس مرچنت ها قرار می دهد. مرچنت ها می توانند وارد سایت شوند و تمام استرداد وجه ها را مشاهده کنند. اگر مرچنت با استرداد وجه موافقت کند، تراکنش بازگردانی می شود، ولی در صورتی که مرچنت مخالف باشد، یک فرایند اختلافی آغاز می شود و در نهایت، اگر

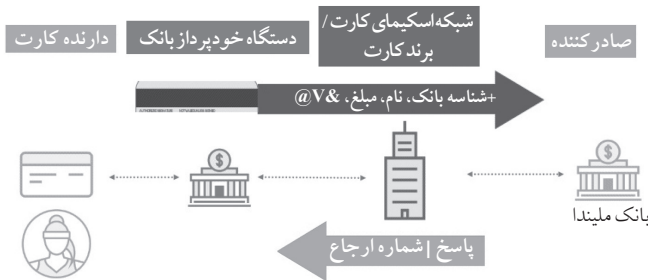
بانک صادرکننده و بانک پذیرنده نتوانند به توافق برسند، شبکه اسکیمای کارت به موضوع ورود می‌کند و تصمیم نهایی را می‌گیرد. از منظر داده، در واقع اختلاف بین بانک‌ها رخ می‌دهد. مرچنت وارد ماجرا نمی‌شود. در فروشگاه یک مرچنت، نامه‌ها، فکس‌ها و ایمیل‌هایی با محتوای درخواست استرداد وجه وجود دارند که از طرف بانک پذیرنده ارسال شده‌اند. این پیام‌ها معمولاً از طریق کانال‌های مجزا، کانال‌های دستی جداگانه و اغلب، از جانب سیستمی فرستاده می‌شوند که برای مجوزدهی و تصفیه تراکنش‌ها مورد استفاده قرار می‌گیرد.

۷. دریافت پول نقد از دستگاه خودپرداز

فراموش نکنید که روزانه، تعداد زیادی تراکنش به شکل نقدی و بدون کارت انجام می شوند، اما اغلب این تراکنش های نقدی نیز با یک تراکنش kartی در دستگاه خودپرداز آغاز می شوند.

در واقع، دارنده کارت به دستگاه خودپرداز مراجعه می کند و با استفاده از کارت، پول نقد را از حسابش برداشت می کند.

تأیید هویت برای پول نقد



شکل ۳۷-۱

این تراکنش ها بسیار شبیه به همان تراکنش های خردی هستند که پیش تر در مورد آنها صحبت کرده ایم. وقتی دارنده کارت، کارتش را وارد دستگاه خودپرداز می کند، یک درخواست تأیید هویت از بانک اپراتور دستگاه خودپرداز به بانک صادرکننده دارنده کارت فرستاده می شود.

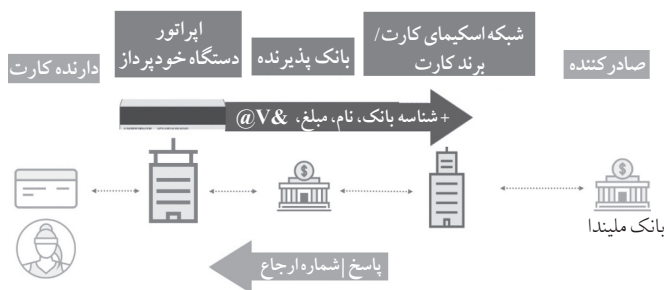
این پیام گاهی اوقات از طریق شبکه اسکیمای کارت ارسال می شود. گاهی نیز پیام

از بانکی به بانک بعدی ارسال می‌شود. در تعدادی از کشورها، یک معادل ملی برای شبکه اسکیمای کارت وجود دارد که فقط برای تراکنش‌های دستگاه خودپرداز به کار گرفته می‌شود.

درست مثل تراکنش‌های پرداخت، وقتی مجوز تراکنش صادر می‌شود، بانک دارنده کارت یک پاسخ به بانک اپراتور دستگاه خودپرداز می‌فرستد؛ اگر پاسخ مثبت باشد، به دستگاه خودپرداز فرمان داده می‌شود تا پول نقد را به دارنده کارت تحویل دهد.

بانک اپراتور دستگاه خودپرداز، در پایان روز، یک پرونده تصفیه تهیه می‌کند و در ساعات اولیه روز بعد، تسویه‌ها را انجام می‌دهد.

تأیید هویت برای پرداخت پول نقد؛ اپراتورهای دستگاه خودپرداز



شکل ۳۸-۱

بعضی مواقع، دستگاه‌های خودپرداز به جای بانک، توسط شرکت‌های شخص ثالث اداره می‌شوند.

در این مواقع، دقیقاً مانند تراکنش‌های خرد، پیام تأیید هویت از دستگاه خودپرداز به اپراتور دستگاه خودپرداز و سپس به بانک پذیرنده انتقال داده می‌شود. عملیات تسویه نیز به شکلی مشابه، روز بعد صورت می‌گیرد.

خلاصه‌ای از نحوه کار تراکنش‌های پرداخت

ما این بخش را با طرح یک پرسش آغاز کردیم. این پرسش بدین ترتیب بود: وقتی یک تراکنش پرداخت را انجام می‌دهید، این تراکنش از چه طریقی در صورت حساب کارت اعتباری شما ظاهر می‌شود و پول به چه روشی از حساب شما برداشت می‌شود.

بانک صادرکننده (یا همان صادرکننده) و شبکه‌های اسکیمای کارت (سه جزئی)، کارت را در اختیار دارندگان کارت قرار می‌دهند.

بانک‌های پذیرنده و شبکه‌های اسکیمای کارت (سه جزئی) تراکنش‌ها را از مرچنت‌ها دریافت می‌کنند.

شبکه‌های اسکیمای کارت (چهار جزئی)، بانک‌های پذیرنده را به صادرکنندگان متصل می‌کنند.

ارائه‌دهندگان خدمات پرداخت و پرداخت یاران، با مرچنت‌ها قرارداد می‌بندند تا تراکنش‌ها را به بانک‌های پذیرنده ارسال کنند.

ما نقش تمامی اعضای فرایند پرداخت را شرح دادیم تا شما دید دقیق‌تری به نحوه کار تراکنش‌ها پیدا کنید. بانک‌های صادرکننده و شبکه‌های اسکیمای کارت شخص ثالث، از قبیل امکس و دیسکاور، کارت‌های پرداخت را به افراد دارنده کارت تحویل می‌دهند. بانک‌های پذیرنده و شبکه‌های اسکیمای کارت شخص ثالث، تراکنش‌ها را از مرچنت‌ها دریافت می‌کنند. شبکه‌های اسکیمای کارت، از جمله ویزا و مسترکارت، در یک مدل چهار جزئی، بانک‌های پذیرنده را به بانک‌های صادرکننده متصل می‌کنند. ارائه‌دهندگان خدمات پرداخت یا پرداخت یاران، بین مرچنت‌ها و بانک‌های پذیرنده قرار می‌گیرند. ما دریافتیم که فرایند پرداخت شامل چند گام است و در هر گام، یک پیام الکترونیکی بین اعضا ردوبدل می‌شود و همین ردوبدل شدن پیام‌هاست که در نهایت، باعث انجام تراکنش می‌شود. هر کدام از این پیام‌ها، دربرگیرنده داده‌های مشخصی هستند و شناخت هدف هر پیام و داده‌هایی که در آن وجود دارد، اولین گام

در تعیین روش حفاظت از داده در برابر سرقت یا دست کاری است.

در مرحله تأیید هویت، کسب و کار پذیرنده کارت با بانک صادرکننده وارد ارتباط می شود تا بررسی کند که آیا پولش به او پرداخت خواهد شد یا خیر؟
در مرحله ثبت، مرجنت تأیید می کند که تراکنش، انجام گرفته است.
در مرحله تصفیه، مرجنت ها و بانک های پذیرنده چکیده ای از تراکنش های روزانه شان تهیه می کنند و صادرکنندگان، بدهی را روی حساب دارنده کارت اعمال می کنند.
در مرحله تسویه، صادرکنندگان پول را به بانک های پذیرنده انتقال می دهند و بانک های پذیرنده پول را به مرجنت پرداخت می کنند.
دارنده کارت می تواند عملیات استرداد وجه را روی تراکنش انجام بدهد (با کمک صادرکننده).

اولین گام در فرایند پرداخت، تأیید هویت نام دارد. این گام زمانی برداشته می شود که مشتری، اقدام به انجام یک تراکنش می کند. مرجنت می خواهد مطمئن شود که پولش را دریافت خواهد کرد، بنابراین یک پیام تأیید هویت را که شامل مقدار زیادی داده است، آماده می کند. گاهی اوقات، مرجنت نیز باید با هدف تأیید اینکه تعهداتش را در برابر مشتری انجام می دهد، تراکنش را ثبت کند. بعد از تأیید هویت، نوبت به پیام های تصفیه می رسد. این پیام ها بین اعضا منتقل می شوند تا همگی بدانند که چقدر به یکدیگر بدهکار هستند. سپس، تسویه انجام می گیرد و پول از بانک های صادرکننده کارت ها، به مرجنت ها ارسال می شود. در قسمت پایانی این بخش، ما آموختیم که تراکنش ها را می توان بازگردانی کرد. هم مرجنت می تواند مبلغ را به دارنده کارت بازپرداخت کند و هم دارنده کارت می تواند عنوان کند که تراکنش را انجام نداده و درخواست استرداد وجه دارد. در انتها، می خواهیم به شما یادآوری کنم که این جهان، بسیار بزرگ است. سیستم پرداخت، طی ۵۰ سال گذشته توسعه زیادی یافته است. در سال های اولیه توسعه این سیستم، مقدار زیادی کاغذ از مرجنت ها به بانک های

پذیرنده، از بانک‌های پذیرنده به شبکه‌های اسکیمای کارت و از شبکه‌های اسکیمای کارت به بانک‌های صادرکننده پست می‌شد. با گذر زمان، این فرایند به سمت پردازش الکترونیکی حرکت کرد. کشورها، سیستم‌های پرداختی را طراحی و توسعه دادند که مختص خودشان بود و استانداردهایی را روی این سیستم‌ها پیاده‌سازی کردند که باز هم به خودشان اختصاص داشت و با سیستم‌های کشورهای دیگر مغایر بود. صرفاً، حدود ۲۰ سال گذشته بوده که کل سیستم پرداخت جهانی، به شکل مناسب و الکترونیکی، به هم متصل شد. امروزه، کشورها، بانک‌های پذیرنده و شبکه‌های اسکیمای مختلف، می‌توانند به شیوه مختص خودشان، به فعالیت بپردازند. بنابراین، درست است که در این بخش، در مورد فرایند کلی پرداخت‌ها صحبت کردیم، ولی همیشه تفاوت‌هایی را بین کشورها و سیستم‌های مختلف مشاهده خواهید کرد. تقریباً در تمامی موارد، عملیات کلی به این شکل است که مرجنت، برای دریافت مبلغ، پیامی را به بانک پذیرنده یا شبکه اسکیمای کارت ارسال می‌کند و این پیام، در نهایت، به دست بانک صادرکننده می‌رسد. کسب آگاهی در مورد محتوای این پیام‌ها، مقصد ارسال آنها و شیوه رسیدن آنها به مقصد، راز حفظ امنیت پرداخت‌ها به شمار می‌رود.



{ بخش دوم }
کدام استانداردهای صنعت
کارت و پرداخت را به کار بگیریم؟ }

۸. مجرمان چگونه از داده‌های کارت و پرداخت نفع می‌برند؟

در این بخش، تمامی استانداردهای مختلف صنعت کارت و پرداخت را زیر ذره‌بین خواهیم برد و بررسی خواهیم کرد که کدام استانداردها برای کار شما مناسب‌تر از بقیه هستند. اما قبل از آن، آیا تا به حال برایتان این سؤال پیش آمده که مجرمان چگونه داده‌های کارت‌های سرقتی را به پول تبدیل می‌کنند؟ آنها این کار را به دو روش انجام می‌دهند؛ اولین روش این است که داده‌های دارنده کارت را به سرقت می‌برند و با استفاده از آنها، کارت‌های کپی شده می‌سازند.

در این روش، مجرمان می‌توانند با کمک کارت‌های کپی، از دستگاه‌های خودپرداز پول نقد بگیرند. در روش دوم، مجرمان با کارت کپی از فروشگاه‌ها خرید می‌کنند و کالاهای خریداری شده را در ازای پول نقد به فروش می‌رسانند یا با به کارگیری داده‌های سرقتی کارت، اقدام به خرید آنلاین کرده و اجناس خریداری شده را می‌فروشند. در تبدیل داده کارت به پول، معمولاً پای بیش از یک مجرم در میان است. در اغلب موارد، دست کم چهار مجرم دست به دست می‌دهند تا داده‌های سرقتی کارت را به پول نقد تبدیل کنند.

مجرم اول، متخصص به سرقت بردن داده کارت از شرکت‌هاست. مجرم دوم، معامله‌گر داده است. او افرادی را پیدا می‌کند تا داده را به آنها بفروشد. مجرم سوم، روی این موضوع کار می‌کند که چگونه داده خریداری شده را به پول تبدیل کند. این گروه از مجرمان، کارت‌ها را کپی می‌کنند یا خرید آنلاین انجام می‌دهند و افرادی را استخدام می‌کنند که کالاها را تحویل بگیرند و سپس، به مجرم تحویل بدهند تا آن را به پول تبدیل کند.

مجرم نهایی، با نام قاطر (Mule) شناخته می‌شود. وظیفه قاطر این است که از دل کالاهای خریداری شده سرقتی، پول نقد بیرون بکشد. از جمله روش‌هایی که قاطر از

آن استفاده می‌کند، این است که به تعداد خیلی زیادی دستگاه خودپرداز مراجعه می‌کند و از حساب پول برداشت می‌کند، یا خرید آنلاین می‌کند و کالاهای سرقتی را به مجرم شماره سه ارسال می‌کند یا حتی به فروشگاه می‌رود، خرید می‌کند و کالاها را به مجرم شماره سه یا فرد دیگری که می‌تواند آن کالا را به پول تبدیل کند، انتقال می‌دهد. در اکثر مواقع، قاطر یک مجرم واقعی نیست؛ بلکه شخصی است که استخدام شده تا از خانه و به صورت اینترنتی کار کند.

چنین فردی ممکن است با خودش فکر کند که یک کارگزار حمل و نقل بسته‌های پستی است، ولی کاری که واقعاً انجام می‌دهد، ارسال مجدد کالاهایی است که با داده‌های کارت‌های پرداخت سرقتی خریداری شده‌اند. اغلب اوقات، قاطرها کسانی هستند که به آسانی دستگیر می‌شوند.

بسته‌های پستی به آدرس واقعی آنها ارسال می‌شوند و مجریان قانون به راحتی می‌توانند به آدرس واقعی آنها مراجعه کنند. اکنون، بیایید نگاهی داشته باشیم به داده‌هایی که یک مجرم، برای رسیدن به مقاصدش، به آنها نیاز دارد و عموماً آنها را به سرقت می‌برد.

پول نقد

برای دریافت پول نقد، به‌طور معمول، باید به دستگاه خودپرداز مراجعه کرد. بدین منظور به یک کارت بانوار مغناطیسی کپی شده نیاز است.

- ترک ۱

پین

مجرمان برای دریافت پول نقد، به یک دستگاه خودپرداز مراجعه می‌کنند. آنها باید کارت‌های کپی شده بسازند و در دستگاه‌های خودپرداز مورد استفاده قرار بدهند، بنابراین باید به طریقی، کل داده‌های ترک ۱ را از بانوار مغناطیسی استخراج کنند. همچنین آنها باید به پین دارنده کارت نیز دسترسی پیدا کنند. اما برای تهیه کالاهای فیزیکی، مجرمان دو گزینه در پیش رو دارند:

کالاهای فیزیکی

فروشگاهی (رودرو، به شکل حضوری)

- کارت بانوار مغناطیسی کپی شده

○ ترک ۱

تجارت الکترونیکی (به شکل غیر حضوری)

- شماره حساب اصلی، تاریخ انقضا، نام
- CVV2 (همیشه درخواست نمی شود)
- آدرس صورت حساب

مجرمان می توانند به یک فروشگاه فیزیکی مراجعه کنند؛ در این صورت، آنها باید با کمک داده های ترک ۱ که از جای دیگری سرقت کرده اند، یک کارت بانوار مغناطیسی کپی شده بسازند. آنها همچنین می توانند به تراکنش تجارت الکترونیکی روی بیاورند. در این روش لازم است آنها به داده هایی که برای تأیید هویت یک تراکنش تجارت الکترونیکی الزامی هستند، دسترسی پیدا کنند. این داده ها عبارت اند از: شماره حساب اصلی، تاریخ انقضا و نام دارنده کارت. در برخی تراکنش های تجارت الکترونیکی، به کد امنیتی CVV2 نیز نیاز است، ولی این گونه نیست که همه مرچنت ها، از مشتری درخواست CVV2 داشته باشند. بعضی از مرچنت ها، در پیامی که برای تأیید هویت به بانک صادر کننده کارت می فرستند، آدرس صورت حساب دارنده کارت را نیز کنترل می کنند.

همان گونه که در بخش قبلی توضیح دادیم، برای انجام هر تراکنش کارت پرداختی، چهار گام باید برداشته شود. این چهار گام عبارت اند از: تأیید هویت، تصفیه، تسویه و بازگردانی تراکنش که به دو طریق استرداد وجه و بازپرداخت انجام می شود. طی چهار گام مذکور، داده بین مرچنت ها، بانک ها و شبکه های اسکیمای کارت به گردش در می آید. در گام تأیید هویت، بیشترین مقدار داده منتقل می شود. در این گام، بانک های صادر کننده بررسی می کنند که آیا می توانند به یک تراکنش مجوز بدهند یا خیر. بنابراین

برای تأیید هویت، باید تمام داده‌های مورد نیاز، برای بانک صادرکننده فرستاده شود. از این رو، قاعدتاً اگر یک مجرم داده‌های مربوط به تأیید هویت را سرقت کند، به تمام داده‌های مورد نیاز برای ارسال درخواست تبه‌کارانه تأیید هویت، دسترسی خواهد داشت. در روش‌های مختلف، برای پذیرش داده کارت، به داده‌های تأیید هویت زیر نیاز است:

ترک ۱

- دستگاه خودپرداز
- فروش حضوری
- خرید سوخت، بلیت و غیره
- شماره حساب اصلی کارت + تاریخ انقضا + CVV2
- تجارت الکترونیکی
- سفارش پستی / سفارش تلفنی (MOTO)
- شماره حساب اصلی + تاریخ انقضا
- تمام داده‌های ترک ۱
- تجارت الکترونیکی یا سفارش پستی / سفارش تلفنی

مجرمان برای دریافت پول نقد از دستگاه خودپرداز یا خرید کالا از فروشگاه‌های فیزیکی، به داده‌های ترک ۱ نیاز دارند. این افراد می‌توانند داده‌های ترک ۱ را از محل دستگاه‌های خودپرداز، فروشگاه‌های خرده‌فروشی یا مکان‌های دیگری که نوار مغناطیسی در آنها کشیده می‌شود، از قبیل پمپ‌بنزین‌ها و دستگاه‌های خرید بلیت حمل و نقل، به سرقت ببرند. مجرمان برای اینکه بتوانند از دستگاه‌های خودپرداز پول بگیرند، به غیر از داده‌های ترک ۱، باید به پین نیز دسترسی داشته باشند. پین را نمی‌توان به روش سرقت داده از درخواست تأیید هویت، به دست آورد؛ بنابراین روش به سرقت بردن پین‌ها را اندکی بعد، در قسمت دیگر کتاب با هم مرور خواهیم کرد. برای انجام تراکنش‌های تجارت الکترونیکی و سفارش پستی، تنها کافی است مجرمان

شماره حساب اصلی، تاریخ انقضا و CVV2 را از خرده‌فروشی که از خدمت تجارت الکترونیکی یا سفارش پستی / سفارش تلفنی پشتیبانی می‌کند، سرقت کنند. در صنعت پرداخت، خرده‌فروشی که خدمت سفارش پستی / سفارش تلفنی را به مشتریان‌شان ارائه می‌دهند، با نام MOTO یا M-O-T-O شناخته می‌شوند. در بعضی مواقع، اگر مجرمان متوجه شوند که یک خرده‌فروش ارائه‌دهنده خدمت تجارت الکترونیکی یا سفارش پستی / سفارش تلفنی، کد امنیتی CVV2 را کنترل نمی‌کند، با مراجعه به منابع مختلف، شماره حساب اصلی و تاریخ انقضا را به دست آورده و شروع به خرید از آن خرده‌فروشی می‌کنند. شیار کارت و وبسایت‌های تجارت الکترونیکی، نمونه‌هایی از این منابع به‌شمار می‌روند. کارت‌های تراشه‌دار، جلوی بسیاری از تقلب‌های حضوری را گرفته‌اند، اما تازمانی که کارت‌های تراشه‌دار در سراسر جهان فراگیر نشده‌اند، مجرمان به سرقت از طریق تراکنش‌های نوار مغناطیسی ادامه خواهند داد. بنابراین در ابتدا بیابید به این موضوع بپردازیم که مجرمان، داده‌های سرقتی از نوار مغناطیسی را از چه طریقی مورد استفاده قرار می‌دهند، سپس تغییر و تحولات حاصل از ظهور فناوری تراشه را مورد بحث قرار خواهیم داد.

بهره‌مندانه‌تر

برای سفارش اینترنتی این کتاب به وبسایت
فروشگاه انتشارات راه پرداخت مراجعه کنید
way2pay.shop



انتشارات راه پرداخت

صنعت کارت و پرداخت

وقتی یک تراکنش انجام می‌دهید، در پشت پرده چه اتفاقی می‌افتد و چه می‌شود که در نهایت، آن تراکنش، روی صورت حساب بانکی شما ظاهر می‌شود. این کتاب نگاهی خواهد داشت برپایمی که بین تمامی اعضای سیستم پرداخت ردوبدل می‌شود و سپس بررسی خواهد کرد که مجرمان چگونه می‌توانند در این پیام‌ها دست ببرند. تعدادی از مهم‌ترین موضوعاتی که در این کتاب به آنها پرداخته می‌شود، عبارت‌اند از: کدام داده‌های کارت و پرداخت در سراسر جهان به گردش درمی‌آیند؟ علت وجود این همه تفاوت در استانداردهای صنعت کارت و پرداخت چیست؟ چه کسی به انطباق هویت شما با هویت ثبت‌شده‌تان اهمیت می‌دهد؟ از چه متر و معیاری برای اعتبارسنجی شما استفاده می‌شود و چگونه می‌توانیم به یک متخصص صنعت کارت و پرداخت تبدیل شویم؟

این کتاب به شما کمک می‌کند تا از این پس، با اعتماد به نفس بیشتری روی پروژه‌های مربوط به صنعت کارت و پرداخت به فعالیت بپردازید.